*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

02/26/2014

**SUBJECT:**

Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in Apple's Mac OS X and Mac OS X Server that could allow remote code execution. Mac OS X and Mac OS X Server are operating systems for Apple computers. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE**

At this time there is no known proof-of-concept code available.

**SYSTEM AFFECTED:**

- Apple Mac OS X 10.7.5
- Apple Mac OS X 10.8.5
- Apple Mac OS X 10.9
- Apple Mac OS X 10.9.1
- Apple Mac OS X Server 10.7.5

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Apple Mac OS X. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- A memory corruption vulnerability affects the 'ATS' component. Specifically, this issue exists in the handling of handling of Type 1 fonts. [CVE-2014-1254]
- A memory corruption vulnerability affects the 'ATS' component. Specifically, this issue exists in the handling of Mach messages passed to ATS. [CVE-2014-1262]
- A security-bypass vulnerability occurs due to an arbitrary free error. Specifically, this issue exists in the handling of Mach messages passed to ATS. [CVE-2014-1255]
- A buffer-overflow vulnerability affects the 'ATS' component. Specifically, this issue exists in the handling of Mach messages passed to ATS. [CVE-2014-1256]
- A security vulnerability affects the 'CFNetwork Cookies' component. Specifically, this issue occurs because Safari fails to properly handle session cookies. [CVE-2014-1257]
- A heap buffer-overflow vulnerability affects the 'CoreAnimation' component. Specifically, this issue exists in CoreAnimation's handling of images. [CVE-2014-1258]
- A security vulnerability affects the 'CoreText' component due to a signedness error. Specifically, this issue exists in the handling of Unicode fonts. [CVE-2014-1261]
- A security vulnerability occurs when using curl to connect to an HTTPS URL containing an IP address. Specifically, this issue occurs because it fails to properly validate the IP addresses against the certificate. [CVE-2014-1263]
- A security-bypass vulnerability affects the 'Date and Time' component. An attacker can exploit this issue to change the system clock. [CVE-2014-1265]
- A remote code execution vulnerability occurs due to a signedness error when handling of 'stsz'. [CVE-2014-1245]
- A remote code execution vulnerability occurs due to an out of bounds byte swapping error when handling of 'ttfo' elements. [CVE-2014-1250]
- A buffer-overflow vulnerability occurs when handling of PSD images. [CVE-2014-1249]
- A buffer-overflow vulnerability occurs when handling of 'ldat'. [CVE-2014-1248]
- A memory corruption vulnerability exists in the handling of 'dref' atoms. [CVE-2014-1247]
- A buffer-overflow vulnerability occurs when handling of 'ftab'. [CVE-2014-1246]
- A memory corruption issue exists in QuickLook's handling of Microsoft Office files. [CVE-2014-1260]
- An unauthorized access vulnerability due to improper handling of ACLs. [CVE-2014-1264]
- A buffer overflow vulnerability exists in the handling of file names. [CVE-2014-1259]

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites, unknown users, or suspicious emails.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

**REFERENCES:**

**Apple:**

http://lists.apple.com/archives/security-announce/2014/Feb/msg00000.html

**Security Focus:**

http://www.securityfocus.com/bid/65777

http://www.securityfocus.com/advisories/31529

**CVE:**

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1254

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1262

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1255

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1256

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1257

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1258

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1261

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1263

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1265

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1245

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1250

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1249

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1248

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1247

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1246

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1260

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1264

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1259